POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS

CARTÓRIO DO RCPN DO 1º DISTRITOI, REGISTRO DE IMÓVEIS, RTD, RCPJ DE ANGRA DOS REIS/RJ

SUMÁRIO

1. OBJETIVOS

Esta política tem como objetivo principal orientar o tratamento de todas as espécies de dados pessoais tratados pelo Cartório do RCPN do 1º Distrito, Registro de Imóveis, RTD e RCPJ de Angra dos Reis/RJ, a partir dos seguintes objetivos específicos:

a. Estabelecer as diretrizes gerais para o tratamento dos dados pessoais coletados pela serventia, abarcando e unificando todas as demais políticas;
b. Proteger os direitos dos titulares dos dados tratados, tais como usuários dos serviços, colaboradores, prestadores de serviço externos e outras pessoas com as quais a serventia se relaciona;
c. Estar em conformidade com a Lei Geral de Proteção de Dados (LGPD), os provimentos das corregedorias e melhores práticas aplicáveis;
d. Proteger a serventia do risco de incidentes de segurança, violações de dados e responsabilizações administrativas e civis.

2. DEFINIÇÕES

A fim de possibilitar uma plena compreensão desta política, faz-se necessário delimitar alguns conceitos presentes nesta política. Veja-se:

a. **Alta Direção**: termo é o tecnicamente utilizado no compliance para designar os responsáveis pela gestão estratégica das organizações. No caso dos cartórios, a Alta Direção é centralizada na pessoa do agente delegado e seus substitutos. A adesão da Alta Direção é fundamental para o sucesso da implementação da LGPD;

b. **Banco de dados:** termo é o tecnicamente utilizado no compliance para designar os responsáveis pela gestão estratégica das organizações. No caso dos cartórios, a Alta Administração é centralizada na pessoa do agente delegado, construído com o fim de atender a uma atividade específica;

c. **Confiabilidade**: propriedade das informações que são íntegras, disponíveis e confidenciais;

d. **Confidencialidade**: informações de acesso restrito e armazenadas com proteção suficiente para que apenas as pessoas autorizadas podem acessá-las;

e. **Integridade**: informações que mantém sua utilidade, precisão, consistência atualidade e autenticidade;

f. **Disponibilidade**: informações que são acessíveis quando é necessário, ou seja, diz respeito à capacidade de que as informações sejam consultadas a qualquer momento. Pode-se garanti-la pela proteção e organização do banco de dados;

g. **Incidente de segurança com dados pessoais**: evento adverso que coloque em risco a confiabilidade das informações, tais como acesso não autorizado, destruição, perda, alteração ou qualquer forma de tratamento de dados inadequada;

h. **Sistema de Gestão de Privacidade de Dados Pessoais (SGPD):** designa um conjunto de atividades direcionadas para que uma organização identifique seus objetivos, determine os processos e recursos necessários para os atingir os coloque em operação dentro de um ciclo de melhoria contínua. Envolve processos, políticas e pessoas (Alta Direção, equipe, fornecedores), fornecendo diretrizes para a implementação, manutenção e melhoria contínua para a proteção de dados dentro do contexto da atividade de tratamento;

i. **Uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, ou entre entes privados;

j. **Interoperabilidade de dados:** característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.

3. PRINCÍPIOS DE PROTEÇÃO DE DADOS

A serventia está empenhada em seguir as obrigações trazidas pela LGPD, a partir dos seguintes princípios:

a. a interpretação da LGPD e regulamentos de proteção de dados devem ser realizada em harmonia com a legislação notarial e de registro, devendo se pautar sobretudo pela regulamentação do Conselho Nacional de Justiça (CNJ) e da Corregedoria-Geral da Justiça estadual;
b. todas as atividades de tratamento devem ser legitimadas em uma das bases legais previstas nos artigos 7º e 11 da LGPD, bem como pautadas na persecução do interesse público, com o objetivo de cumprir as atribuições legais do serviço;
c. os dados pessoais devem ser coletados para fins legítimos, específicos e explícitos, sendo vedada a sua utilização para finalidades diversas das informadas ao titular;
d. os dados pessoais devem ser mantidos pelo tempo necessário para atender à finalidade para os quais foram coletados, com sua eliminação após encerrada tal finalidade, salvo necessidade de armazenamento para cumprimento de dever legal;
e. os dados pessoais devem ser armazenados de forma a garantir sua qualidade, isto é, exatidão, clareza, relevância e atualização;
f. durante todo o ciclo de vida dos dados, a serventia empenhará esforços para garantir sua segurança, por meio de medidas preventivas e reativas, conforme descrito na **Política de Segurança da Informação**.

4. PROCESSAMENTO LEGAL, JUSTO E TRANSPARENTE

Frente às necessárias mudanças nos processos da serventia, acarretadas pelo posicionamento adotado em internalizar os valores da LGPD na cultura organizacional, os esforços implantados resultam em um processamento de dados legítimo e transparente, de modo que:

a. O encarregado de dados assumirá a responsabilidade pela conformidade contínua do

cartório com esta política, por meio de programa de conscientização. Os colaboradores devem requisitar ajuda ao encarregado para sanar quaisquer dúvidas relacionadas à proteção de dados;

b. Para garantir um processamento de dados em conformidade com a lei, o cartório manterá atualizado seu **Inventário de Dados e Pessoais**, que indica o ciclo de vida dos dados e as bases legais que legitimam o tratamento;
c. O cartório dever garantir que os titulares tenham ciência de quais dados seus estão sendo tratados, a finalidade do tratamento e como podem exercer seus direitos perante a serventia. Para tanto, a serventia deve manter atualizada sua **Política de Privacidade**, bem como os demais documentos informativos (termos de uso do site, política de cookies, aviso de câmeras, dentre outros). Tais documentos devem ser divulgados no site e no espaço físico do cartório, por meio de cartazes;
d. Quaisquer solicitações dos titulares de dados deverão ser respondidas conforme indicações da **Política de Atendimento**. Caso a solicitação seja efetuada verbalmente, deverá ser atendida imediatamente. Se isso não for possível, deve-se informar à pessoa que a demanda será encaminhada ao encarregado de dados. Caso a solicitação seja efetuada em outro e-mail da serventia, deve ser encaminhada ao e-mail do encarregado, com indicação ao solicitante de que a demanda foi encaminhada internamente;
e. Feita a solicitação no canal de atendimento – ou encaminhada de outros setores –, caberá ao encarregado de dado a análise da pertinência do pedido. Tal análise deverá ser realizada da maneira mais breve possível, dentro dos prazos recomendados na **Política de Atendimento**;
f. Se o consentimento for a base legal adequada para a atividade de tratamento, as evidências que comprovem sua concessão devem ser devidamente arquivadas. Além disso, deve ser facultado ao titular a possibilidade de revogar a autorização a qualquer tempo, mediante solicitação pelo canal de atendimento do encarregado de dados.

5. RESPONSABILIDADES

Todos aqueles que manipulam dados pessoais em nome da serventia – interna ou externamente – devem garantir que o fazem em observância a esta política e aos princípios de privacidade de dados aqui presentes e trazidos pela LGPD. Algumas funções possuem responsabilidades-chave:

a. membros da **Alta Direção** – a saber, titular e substitutos – são responsáveis por:

   i. Assegurar o cumprimento desta política;

   ii. Assegurar que os recursos necessários para o Sistema de Gestão de Privacidade de Dados Pessoais (SGPD) estejam disponíveis;

   iii. Comunicar a importância do SGPD;

   iv. Assegurar que esta Política alcance os seus objetivos e resultados pretendidos;

   v. Promover a melhoria contínua do SGPD;

   vi. Apoiar os papéis relevantes no ciclo de gestão do SGPD.

b. Os responsáveis pelas áreas **Administrativa e Financeira** da serventia, que:

   i. Manipular dados de contratos;

   ii. Gerenciar pagamentos e recebimentos;

   iii. Analisar propostas comerciais de fornecedores;

   iv. Realizar contato com usuários, fornecedores e colaboradores, usando diversos meios de comunicação, como e-mail, telefone e aplicativos de mensagens.

c. O **Encarregado de dados** é responsável por:

   i. Manter a administração da serventia atualizada em relação a responsabilidades, riscos e questões conexas a privacidade de dados;

   ii. Revisar periodicamente políticas e procedimentos relacionados à privacidade de dados;

iii. Fornecer treinamento adequado em proteção de dados para os indivíduos contemplados nesta política;

iv. Responder a questões sobre privacidade de dados feitas por colaboradores ou outro indivíduo pertinente;

v. Lidar com requisições de informação, alteração, exclusão, portabilidade e acesso a dados pessoais feitas pelos titulares;

vi. Avaliar (e aconselhar a Direção acerca de) qualquer contrato ou acordo com terceiros que manipulem dados sensíveis controlados pela serventia.

d. A Área de **Tecnologia da Informação** é responsável por:

i. Garantir que todos os sistemas, serviços e equipamentos usados para o armazenamento de dados possuam padrões aceitáveis de segurança;

ii. Realizar checagens e varreduras periódicas para garantir que os respectivos hardwares e softwares de segurança estão funcionando de forma apropriada;

iii. Avaliar qualquer serviço ofertado por terceiro para armazenar ou tratar dados pessoais (e seu nível de segurança), como, por exemplo, serviços de computação em nuvem.

6. MINIMIZAÇÃO DE DADOS PESSOAIS

Para atendimento da finalidade pública, o tratamento de dados pessoais atribuído à serventia observa os princípios da LGPD, as hipóteses autorizativas, e operacionaliza os direitos dos titulares. Tendo isso em consideração, sua atuação está pautada:

a. Com base no princípio da necessidade, devendo garantir que os dados pessoais sejam precisos, relevantes e limitados ao que é necessário para cumprimento das finalidades que legitimam sua coleta;
b. Quando cabível, técnicas para anonimização e pseudoanonimização deverão ser

utilizadas para elevar a segurança dos dados tratados;

c. Assim que não mais persistir a finalidade para qual o dado pessoal foi coletado, e não mais existir qualquer obrigação legal ou regulatória, ou mesmo interesse jurídico em mantê-lo, este será prontamente excluído da base de dados pessoais tratados pela serventia;
d. Para garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário, a serventia deve estabelecer à temporalidade de armazenamento das informações, além de estabelecer procedimentos para descarte seguro, de modo a tornar os dados excluídos irrecuperáveis. Essa matéria é tratada em detalhes na **Política de Gestão Documental e Descartes**, baseada no Provimento nº 50/2015 do CNJ;
e. Dados pessoais devem ser armazenados no menor número possível de locais diversos entre si.

7. SEGURANÇA E CONFIABILIDADE DAS INFORMAÇÕES

Segurança e confiabilidade das informações são dois pilares de grande relevância para a proteção de dados pessoais. Uma serventia com um sistema atualizado e um projeto de conformidade implementado também depende da junção de pessoas que respeitem as regras e processos, por isso a mitigação dos riscos engloba:

a. Que os dados armazenados fisicamente sejam arquivados em local seguro, que impeça incidentes de segurança. De igual modo, que seja restrito o acesso dados armazenados digitalmente por meio de ferramentas de sistema, como acesso por login e senha e escalas de permissão por grupos de acesso. Os demais cuidados a serem tomados neste sentido estão descritos na **Política de Segurança da Informação** e no **Manual de Conduta**;
b. Que os dados pessoais não devem ser compartilhados informalmente. Caso necessitem de ter acesso à informação confidencial, o empregado deve requisitar tal acesso ao seu superior;

c. Que qualquer indivíduo que acesse informações que não fazem parte do escopo de trabalho deve **comunicar imediatamente** tal fato à área de tecnologia da informação, bem como ao encarregado de dados;

d. Que é responsabilidade de todos que manuseiam dados pessoais tomar os cuidados adequados para manter preservada sua integridade;

e. Convém que a serventia continuamente invista em tecnologias avançadas para que o acervo seja armazenado em ambiente atualizado;

f. Soluções adequadas para prevenção e recuperação de incidentes, já devidamente implementadas, devem ter sua adequação avaliada periodicamente. Além disso, convém que as tecnologias empregadas sejam constantemente avaliadas.

8. COMPARTILHAMENTO DE DADOS PESSOAIS

Segundo a LGPD, há situações em que os dados pessoais podem ser comunicados, difundidos, transferidos ou interconectados. O uso compartilhado de dados na serventia ocorre mediante previsão legal ou consentimento do titular, e sempre considerará que:

a. As informações do banco de dados deverão ser mantidas em formato interoperável e estruturado para o uso compartilhado;

b. A LGPD confere permissão geral para o uso compartilhado de dados entre órgãos do Poder Público, mas condiciona tal atividade ao atendimento das finalidades específicas de execução de políticas públicas e atribuição legal pelos destinatários. Assim, a serventia deverá analisar solicitações de compartilhamento são legítimas, buscando assistência junto a seu encarregado de dados e demais consultores, quando necessário;

c. A LGPD prevê como regra geral a vedação ao compartilhamento de dados com entes privados, mas estabelece uma série de exceções em que ele é devido:

    i. Para execução descentralizada de atividade pública que exija o uso

compartilhado de dados, observado o disposto na Lei de Acesso à Informação;

ii. nos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD;

iii. quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

iv. na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

d. Dados pessoais não devem ser compartilhados com pessoas sem autorização de acesso a eles, seja de fora ou de dentro da serventia;
e. Todos os terceiros que manipulem os dados pessoais em nome da serventia deverão possuir padrões de segurança adequados para tal, além de observar os mesmos princípios de privacidade de dados que pautam a conduta da serventia.

9. TRATAMENTO DE DADOS DOS COLABORADORES

Para o cumprimento de seus deveres legais e para a Administração, a Serventia coletará informações de colaboradores durante o processo de contratação e no decorrer de todo contrato de trabalho.

a. As informações referidas no caput desta cláusula constam abaixo delimitadas:
   Dados do Colaborador.
   Dados dos Dependentes.
b. Os dados pessoais acima listados serão tratados pela Serventia para as seguintes finalidades:
   i. Cumprimento de obrigações regulatórias ou legais, dentre elas as trabalhistas, previdenciárias, fiscais e tributárias, incluindo o disposto em Acordos ou

Convenções Coletivas da categoria do Colaborador e do Empregador;

ii. Viabilização de relação de trabalho, praticando atos diversos. A título de exemplo: formalização e registros obrigatórios na CTPS física e/ou digital; procedimentos de admissão, execução e rescisão do Contrato de Trabalho; registros em livros, fichas ou arquivos eletrônicos da Serventia; registro e pagamento do Fundo de Garantia por Tempo de Serviço (FGTS); registro e pagamento de contribuições previdenciárias; emissão de recibos de pagamento de salário, férias, décimo-terceiro salário, bônus e outros valores devidos ao colaborador; aquisição do vale-transporte; contratação de plano de assistência médica e/ou odontológica; registro e autorização de uso de sistemas internos, softwares e demais funcionalidades relativas à função; e criação e uso de e-mail corporativo;

iii. Manter contato entre as partes, em razão da relação de trabalho e dos efeitos jurídicos dela decorrentes;

iv. Manter a segurança das instalações da Serventia, evitando fraudes e quebras de confidencialidade.

c. Para as finalidades listadas acima, a Serventia poderá compartilhar os dados pessoais do colaborador com outros agentes de tratamento de dados, incluindo, mas não se limitando, aos seguintes destinatários:

i. escritório de contabilidade;

ii. escritório de contabilidade de advocacia;

iii. empresas prestadoras de serviços de software e gestão;

iv. operadoras de planos de assistência médica e odontológica;

v. empresas emissoras de vale-transporte, vale-refeição e vale-alimentação;

vi. instituições financeiras;

vii. órgãos e entes públicos, tais como o Instituto Nacional de Seguro Social (INSS);

viii. Ministério Público do Trabalho de Emprego (MPTE);

ix. Serviços Especializados em Engenharia de Segurança e Medicina do Trabalho (SESMT).

10. DISPOSIÇÕES FINAIS

Este documento será avaliado anualmente, podendo ser alterado a qualquer tempo e critério. As pessoas que violarem esta política estarão sujeitas às medidas legais e/ou disciplinares cabíveis.